

# Network Security Forum 2014

ミニパネル

電子署名をめぐる国内外の最新動向

## 「電子署名の今後に向けて」 ～スキルアップTFの活動から～

宮地 (miyachi@langedge.jp)

電子署名WGサブリーダー/スキルアップTFリーダー  
(有限会社ラング・エッジ)

2014年1月29日

# 話の前にスキルアップTF



電子署名の今後の動向を調査・勉強・開拓する  
未来志向のタスクフォースです。

1. 勉強会でWG/TFメンバーのスキルアップ
2. 新しいトレンドや情報をキャッチアップ
3. 電子署名プログラマへの情報や環境提供

2013年度は既に6回勉強会を開催。  
興味があれば外部からも講演者を招へい。  
新しい事に挑戦します！

# スキルアップTF勉強会テーマ



## 第1回：7月：長期署名入門

講師＞電子署名WGオールスター 宮崎氏、佐藤氏、石本氏、西山氏、宮地

## 第2回：8月：クラウド署名とHSM

講師＞タレス・ジャパン 住田氏、セーフネット/JIPDEC客員研究員 亀田氏、他

## 第3回：9月：jsrsasign / jsjws 勉強会

講師＞富士ゼロックス 漆嵐氏

補足＞JavaScriptによるRSA/PKIモジュールとJSON署名

## 第4回：10月：PDF電子署名仕様入門

講師＞ラング・エッジ 宮地

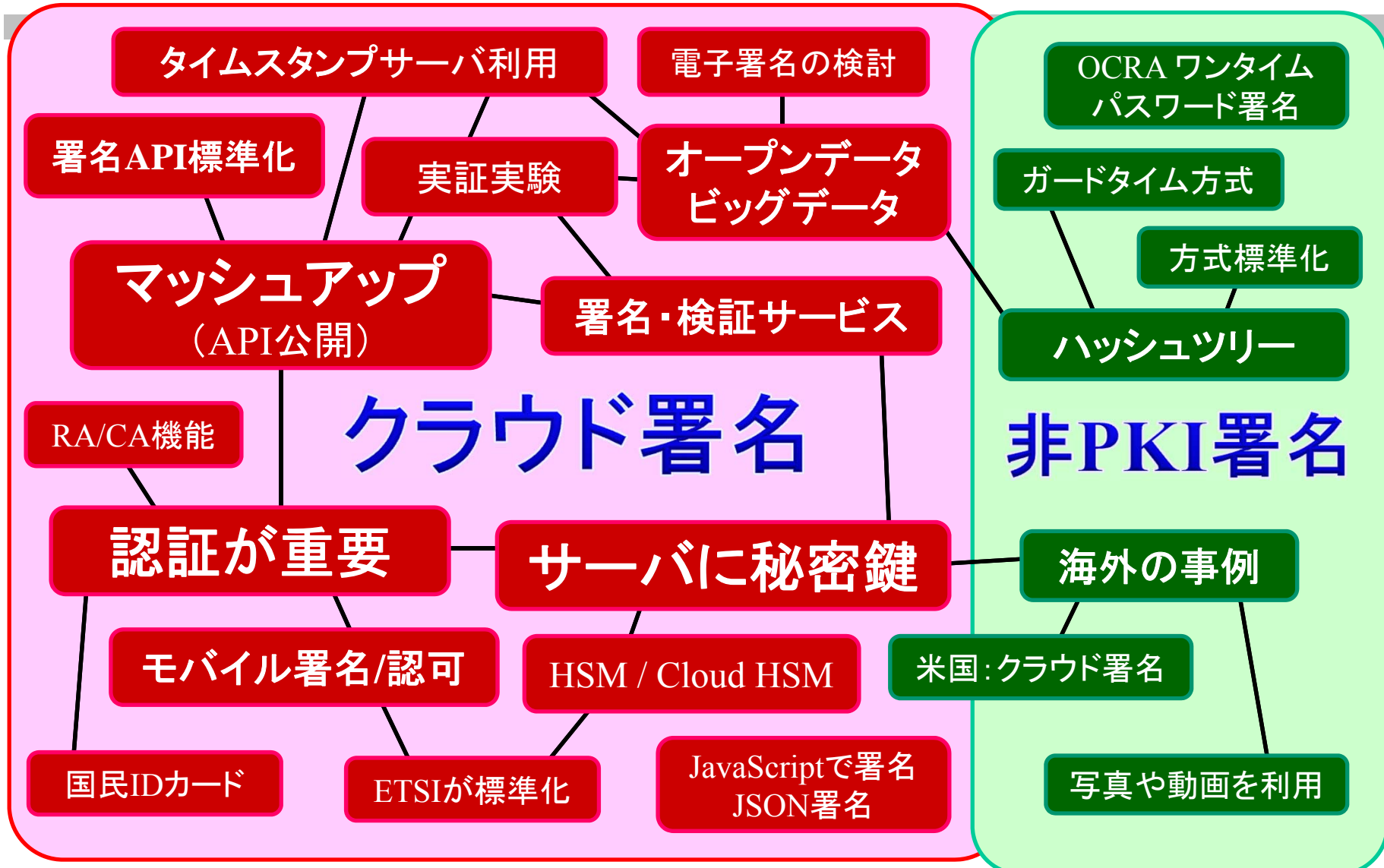
## 第5回：11月：クラウド時代のデータセキュリティ

講師＞ガードタイム 柳原氏

補足＞ガードタイム社による非PKI署名他

## 第6回：1月：電子署名WG合宿ダイジェスト

# 今後のキーワードを俯瞰



# 遊び場プロジェクト



## ～プログラマの為のお試し環境構築～

	CA機能		TSA機能	情報公開	署名機能	検証機能	
証明書・鍵サービス	リポジトリ公開 HTTP   LDAP	OCSP発行	タイムスタンプ発行	ソース他公開	サービス提供	サービス提供	
対話画面による発行	CA証明書は公開 CRLは定期的に更新 出来ればCSP/CP等も	証明書DB またはCRL 連動し発行	CA機能で TSA証明書を準備	各機能実装 情報やサンプルを公開	APIや対話画面を用意して クラウド的にモバイル署名も 考慮して検討する		
OpenSSLのCA機能 認証連携	OpenSSLの 簡易CA機能を利用 画面は作成が必要	OpenSSLで 可能？ ocspオプション利用	 準備完了 FreeTSA	Wiki, Blog GitHub 等	Ruby on Rails 等か CA機能と連携？ FreeXAdES, jsrsasign 等の利用		
証明書・秘密鍵は登録制等にして完全フリーは難しいかも。一応本人確認くらいはする？ OCSPは最初は無くて良いかもしれない。			認定TSAからの提供も歓迎	長期署名サンプル等ノウハウも	クラウド署名の実証実験的にできるとベスト HSM等使えると面白い		
JNSAではかつて「チャレンジPKI <a href="http://www.jnsa.org/mpki/index_j.html">http://www.jnsa.org/mpki/index_j.html</a> 」があった。今は使えない。							

興味を持った技術者がフリーで使えてプラグテストにも使える！

# 参考: FreeTSA (本日は説明無し)



OpenSSLコマンドによる簡単タイムスタンプ(RFC3161)サービス

□ タイムスタンプって面白そうだから使ってみたい！

□ タイムスタンプ クライアントの試験って使えるサーバは？

というような要望に応える為にOpenSSL 1.0.0のコマンドを利用して簡易タイムスタンプサービス(サーバ)の構築手順をまとめた。ラング・エッジのサーバで稼働させて手軽に使えるタイムスタンプサービスを提供中。プロジェクトとしては以下の2つ。なお作るには別途TSA証明書は用意が必要。

作る: FreeTSA Project: 10分でできるタイムスタンプ局


使う: FreeTSA Service: 自由に使えるタイムスタンプ局

➤ 参考 LangEdge Weblog: フリータイムスタンプ局 (FreeTSA) のすゝめ

<http://www.langedge.jp/blog/index.php?itemid=665>

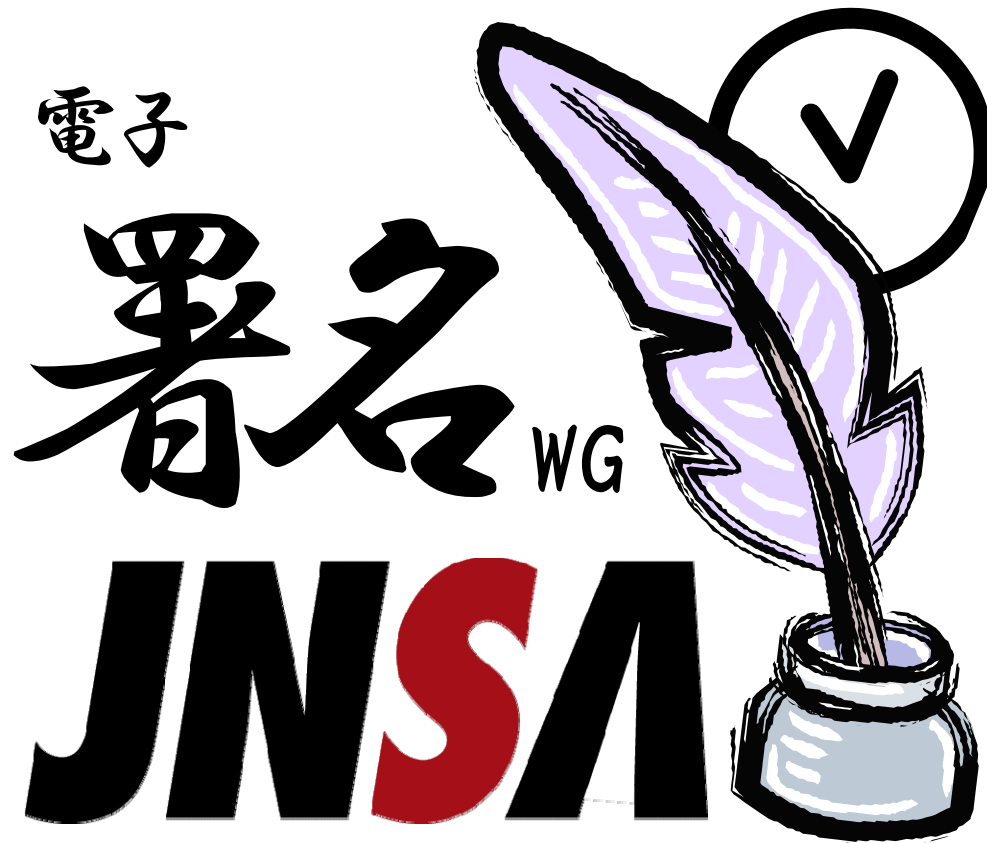
# 電子署名の今後に向けて

- 引き続き、新しいテーマを調査・勉強・開拓
  - 将来性があれば新しいTFの立ち上げ
- 勉強会を利用して実装や開発を（手を動かす）
  - 遊び場プロジェクトの推進
  - フリーソフトやプロジェクトの開発（FreeXAdES等）
- 他WGや他団体との連携（特にクラウド方面）
- 一般のプログラマ・技術者向け勉強会の開催
  - できれば若い電子署名技術者でコミュニティ形成を
- 足りない仕様の検討と標準化
  - 仕様の後追いでは無く先行したい
- 実証実験やプラグテストの実施
- 報告書や資料の作成と公開



若い世代の  
活性化を！

FaceBookページやっています



*Japan Network Security Association  
Electronic Signature Working Group*

最新情報やイベント情報等を公開しています。

<https://www.facebook.com/eswg.jnsa.org>



最後に



---

ご清聴ありがとうございました。



宣伝

クラウド/モバイル署名 & 非PKI電子署名  
詳しくは3月13日の PKI Day 2014 にて！

電子署名WGへの参加者募集中です！